

Appl. No. 10/058,214

Reply to Office Action of: December 12, 2005

**REMARKS**

Applicant wishes to thank the Examiner for reviewing the present application.

Applicant acknowledges the Examiner's indication that claim 8 would be allowable if rewritten in independent form. Each independent claim, namely claims 1, 9 and 10 are amended to include the subject matter of allowable claim 8, and as such, are believed to be in condition for allowance. Remaining dependent claims 2-7 and 11-12 are believed to also be in condition for allowance by virtue of the amendments to independent claims 1, 9 and 10.

**Amendments to the Claims**

Independent claims 1, 9 and 10 are amended inserting "wherein said truncator is  $\frac{\tau^m - 1}{\tau - 1}$ , and wherein  $m$  is the extension degree of a finite field over which said elliptic curve is defined", previously the subject matter of allowable claim 8. Accordingly, claim 8 is cancelled.

No new subject matter is believed to have been added by way of these amendments.

**Claim Rejections – 35 U.S.C. §103**

Claims 1-12 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Kobayashi et al. in view of U.S. Patent No. 5,373,560 to Schlafly.

As indicated above, claim 8 has been deemed allowable by the Examiner if rewritten in independent form, and claims 1, 9 and 10 are hereby amended inserting the allowable subject matter of claim 8.

Accordingly, Applicant respectfully submits that the Examiner's rejections under 35 U.S.C. §103(a) are thereby rendered moot, and that claims 1, 9 and 10, and claims 2-7 and 11-12, dependent thereon, patentably distinguish over Kobayashi in view of Schlafly.

**BEST AVAILABLE COPY**

Appl. No. 10/058,214

Reply to Office Action of: December 12, 2005

Summary

In view of the foregoing, Applicant respectfully submits that all pending claims, namely claims 1-7 and 9-12 patentably distinguish over the prior art cited by the Examiner and as such are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



John R.S. Orange  
Agent for Applicant  
Registration No. 29,725

Date: Mar 9th, 2006

BLAKE, CASSELS & GRAYDON LLP  
Suite 2800, P.O. Box 25  
199 Bay Street, Commerce Court West  
Toronto, Ontario M5L 1A9  
CANADA

Tel: 416.863.3164  
JRO/BSL

BEST AVAILABLE COPY